PERFORMANCE AUDIT
OF THE

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF TREASURY

June 2000

27-590-99

EXECUTIVE DIGEST

AUTOMATED INFORMATION SYSTEMS

INTRODUCTION

This report, issued in June 2000, contains the results of our performance audit* of the Automated Information Systems, Department of Treasury.

AUDIT PURPOSE

This performance audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*.

BACKGROUND

The Information Technology Services Division's (ITSD's) function is to develop, implement, and operate the Department's automated information systems and to provide assistance with these functions. ITSD provides data processing services to the Department. These services include local area network* (LAN) administration, system development and modifications, and microcomputer support. For fiscal year 1998-99, ITSD had appropriations of $11,550,000 and was authorized 167 full-time equated positions.

The Joint Electronic Filing (JELF) System* and the RECON-Plus System* are information processing systems. The Department uses the JELF System to process, store, and retrieve electronic tax returns. For tax

** See glossary at end of report for definition.*

year 1998, the Department processed approximately 621,000 electronic returns, a 46% increase over 1997. The Department uses the RECON-Plus System to reconcile bank accounts with the State's accounting records. For the month of June 1999, RECON-Plus processed approximately 850,000 transactions to reconcile a cash balance of approximately $3 billion.

AUDIT OBJECTIVES AND CONCLUSIONS

Audit Objective: To assess the effectiveness of the Department's general controls over the management, security, and program changes of its LAN-based automated information systems.

Conclusion: The Department's general controls over management, security, and program changes of its LAN-based automated information systems were limited in their effectiveness and should be improved. Our assessment did not disclose any material conditions*; however, we noted reportable conditions* related to a comprehensive information systems security program, LAN user access controls, LAN physical security controls, LAN backup and recovery controls, software licensing agreements controls, and program change controls (Findings 1 through 6).

Audit Objective: To assess the effectiveness of the Department's internal control* over the information system that supports electronic filing of tax returns.

Conclusion: The Department's internal control over information systems that support electronic filing was reasonably effective. Our assessment did not disclose any material conditions; however, we noted reportable

** See glossary at end of report for definition.*

conditions related to JELF access controls and software approval procedures (Findings 7 and 8).

Audit Objective: To assess the effectiveness and efficiency of the Department's internal control over the information system used to reconcile bank accounts with the State's accounting records.

Conclusion: The internal control over the Department's system used to reconcile bank accounts with the State's accounting records was reasonably effective. Our assessment did not disclose any material conditions; however, we noted reportable conditions related to RECON-Plus user access controls and RECON-Plus system documentation (Findings 9 and 10).

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the information processing and other records of the Automated Information Systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Our methodology included examination of the Department's information processing and other records primarily for the period October 1998 through August 1999. Also, we identified the Department's automated information systems and performed a risk assessment of each system. We used this assessment to determine the systems to audit and the extent of our detailed analysis and testing. We performed an assessment of internal control pertaining to (a) general controls over the management, security, and program changes of LAN

based systems, and (b) application controls over the JELF System and the RECON-Plus System. We evaluated and reported on the results of our testing.

AGENCY RESPONSES

Our audit report contains 10 findings and 10 corresponding recommendations. The Department's preliminary response indicated that it agreed with all of the recommendations.

June 20, 2000

Mr. Mark A. Murray
State Treasurer
Treasury Building
Lansing, Michigan

Dear Mr. Murray:

This is our report on the performance audit of the Automated Information Systems, Department of Treasury.

This report contains our executive digest; description of agency; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This page left intentionally blank.

TABLE OF CONTENTS

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF TREASURY

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Information Technology Services Division (ITSD)

ITSD is an organizational component of the Bureau of Administrative Services, Department of Treasury. ITSD's function is to develop, implement, and operate the Department's automated information systems and to provide assistance with these functions. ITSD also provides end-user computing, computer programming, data entry, and mainframe scheduling services to the Department as well as administering the Department's local area network. For fiscal year 1998-99, ITSD had appropriations of $11,550,000 and was authorized 167 full-time equated positions.

Joint Electronic Filing (JELF) System

The Department uses the JELF System to process, store, and retrieve electronic tax returns. The Michigan Department of Treasury has joined with the Internal Revenue Service (IRS), U.S. Department of Treasury, to provide for joint electronic filing of income tax returns. The federal - State joint electronic filing program allows taxpayers to file both federal and State returns electronically through tax practitioners or approved tax software*. The State return must be filed with a federal return because the Department relies on the IRS to receive and transfer the State income tax return to the Department for processing.

The JELF System is a client-server* system that was developed and piloted in-house in 1989. Since 1993, the Department has accepted income tax returns filed by tax practitioners through the federal electronic filing service. In 1997, electronic filing was made available to individuals through the Internet. For tax year 1998, the Department processed approximately 621,000 electronic returns, a 46% increase over 1997.

RECON-Plus System

The Department is responsible for reconciling the cash balances reported by the banks with the cash balance in the State's accounting records. To simplify this process, the Department purchased RECON-Plus. RECON-Plus is a client-server application designed to reduce the time required to match bank and book entries and to increase the number of items matched without user intervention. Users can devote their time to

* *See glossary at end of report for definition.*

researching and resolving unmatched items for more accurate and timely reconciliations.

The Department purchased RECON-Plus in 1998. The application was put into production in October 1998, with an expected transition period lasting through fiscal year 1998-99. For the month of June 1999, RECON-Plus processed approximately 850,000 transactions to reconcile a cash balance of approximately $3 billion.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit of the Automated Information Systems, Department of Treasury, had the following objectives:

1. To assess the effectiveness of the Department's general controls over the management, security, and program changes of its local area network (LAN) based automated information systems.

2. To assess the effectiveness of the Department's internal control over the information system that supports electronic filing of tax returns.

3. To assess the effectiveness and efficiency of the Department's internal control over the information system used to reconcile bank accounts with the State's accounting records.

Audit Scope

Our audit scope was to examine the information processing and other records of the Automated Information Systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Department's information processing and other records primarily for the period October 1998 through August 1999. Our work was performed during February through August 1999. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified the Department's automated information systems and performed a risk analysis of each system to identify systems with the highest risk. Our risk assessment considered the last time a system was audited and the critical nature of the

information processed through the system. We used this analysis to determine the systems to audit and the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

We performed an assessment of internal control pertaining to: (a) general controls over the management, security and program changes of LAN-based automated information systems, and (b) application controls, which included data origination, data input, data processing, and data output for the JELF System and the RECON-Plus System. Specifically, we assessed:

a. Effectiveness of General Controls:

(1) We analyzed controls over the management of the Department's LAN-based automated information systems.

(2) We examined procedures for developing and implementing program changes to LAN-based systems.

(3) We observed and assessed the security of the LAN, including physical security, backup, and access controls.

b. Effectiveness of Internal Control Over the Information System that Supports Electronic Filing of Tax Returns:

(1) We evaluated controls over access and use of the automated information system.

(2) We assessed and documented internal control over data input, data processing, and data output. Also, we conducted tests to determine whether the controls were working as intended.

(3) We reviewed the effectiveness of management's strategy for expanding participation in the electronic filing program.

c. Effectiveness and Efficiency of the Department's Internal Control Over the Information System Used to Reconcile Bank Accounts with the State's Accounting Records:

(1) We evaluated controls over access and use of the automated information system.

(2) We assessed and documented internal control over data input, data processing, and data output. Also, we conducted tests to determine whether the controls were working as intended.

(3) We assessed the efficiency of the system in completing reconciliations.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

Agency Responses

Our audit report contains 10 findings and 10 corresponding recommendations. The Department's preliminary response indicated that it agreed with all of the recommendations.

The agency preliminary response which follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of Treasury to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF GENERAL CONTROLS

COMMENT

Background: General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. Although general controls are normally independent of individual computer applications, they provide the framework within which many different applications are processed. Therefore, weaknesses in general controls can adversely affect all of a department's automated information systems.

Audit Objective: To assess the effectiveness of the Department of Treasury's general controls over the management, security, and program changes of its local area network (LAN) based automated information systems.

Conclusion: The Department's general controls over management, security, and program changes of its LAN-based automated information systems were limited in their effectiveness and should be improved. Our assessment did not disclose any material conditions; however, we noted reportable conditions related to a comprehensive information systems security program, LAN user access controls, LAN physical security controls, LAN backup and recovery controls, software licensing agreement controls, and program change controls.

FINDING

1. Comprehensive Information Systems Security Program

The Department had not established a comprehensive information systems security program.

A comprehensive security program should include detailed policies and procedures for safeguarding all agency information systems resources, comprehensive periodic risk assessments, and resources for monitoring information systems activity.

The Department had not performed a comprehensive risk assessment. Risk assessments help to identify system risks and appropriate security safeguards. They also help ensure that the computer security systems are cost-effective, up-to-date, and responsive to threats. Without periodic, comprehensive risk assessments, security risks may go undetected and uncorrected.

The Department had assigned the network security function to the manager responsible for administering the Department's networks. Although the network administrators have a role to play in maintaining the security of network resources, overall network security should be independent. An independent security officer should monitor system access and educate users about the importance of information systems security. Security officer duties also should include establishing a security program, developing and enforcing security policies and procedures, and monitoring system-recorded security activities and violations.

The Department's lack of a comprehensive security program for safeguarding agency information system resources contributed to the following control weaknesses:

a. The Department had not established effective LAN user access controls over data and application program files (Finding 2).

b. The Department had not established effective physical security controls over LAN resources (Finding 3).

c. The Department had not established effective LAN backup and recovery controls (Finding 4).

d. The Department had not established effective access controls for the Joint Electronic Filing (JELF) System (Finding 7).

e. The Department had not established effective access controls over RECON-Plus (Finding 9).

f. The Department had not taken the necessary action to make certain that the personal computer used for electronic file transmissions was secure.

The Department should incorporate all its information systems into the development of a comprehensive security program. Without a comprehensive security program, management cannot ensure that the Department's internal control is operating as intended and that sensitive information will remain confidential.

RECOMMENDATION

We recommend that the Department establish a comprehensive information systems security program.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us that Information Technology Services Division (ITSD) and Office of Internal Audit will establish a comprehensive information systems security program by September 30, 2000.

FINDING

2. LAN User Access Controls

The Department had not established effective LAN user access controls over data and application program files.

Effective LAN access controls establish accountability primarily through the use of usercodes that identify an individual and passwords, which authenticate the individual. Effective controls also include granting access to data and application program files only to the extent necessary for individuals to perform their assigned duties.

Our review of LAN access controls disclosed that the Department had not developed comprehensive policies and procedures for LAN administration. As a result, the following LAN control weaknesses occurred:

a. The Department did not disable the usercodes of employees who had terminated employment, had transferred to another department, or were on

medical leave. We reviewed 20 of 55 active usercodes that had not logged into the network in the past 90 days and identified:

(1) Two individuals who did not have a human resource employment file and who could not be identified by Department personnel.

(2) Five individuals who had resigned, had transferred to another department, or were on a medical leave of absence.

Allowing former employees and those on leave to access the Department's LAN could result in unauthorized access to LAN resources.

b. The Department did not effectively control its LAN usercodes and passwords. The Department did not:

(1) Require all usercodes to have passwords.

(2) Require each user to have a unique usercode. Generic usercodes had been shared by numerous individuals.

Requiring users to have unique usercodes and passwords reduces the risk of unauthorized access to the LAN and allows management to maintain accountability.

c. The Department did not restrict network users to only one connection. Our review disclosed that 37 users were allowed five or more concurrent connections. Allowing users more than one concurrent connection increases the risk that users will leave their computers unattended while signed onto the LAN.

d. The Department did not automatically disconnect computer network connections after a reasonable period of inactivity. This could result in unauthorized system access at unattended computers. The Department of Management and Budget (DMB) Administrative Guide procedure 1310.02 requires that network connections be automatically disconnected if left unattended for a specific period of time.

e. The Department did not ensure that computer security agreements were properly completed before granting users access to the network. A properly executed security agreement assures management that users are aware of their responsibilities regarding license restrictions, software usage, and confidentiality of information. We reviewed 40 of the Department's LAN usercodes and noted:

(1) Authorization forms were not available for 19 of the 40 usercodes.

(2) One form was missing the employee's signature and the approving supervisor's signature.

(3) Eight authorization forms did not include the usercodes assigned to the individuals.

(4) Eight authorization forms were missing the LAN manager's signature.

f. The Department did not restrict the LAN administrator usercode and administrator access rights to appropriate users. The LAN administrator usercode and administrator access rights provide the capability to manage network resources. This capability should be restricted. We noted that:

(1) Three network managers knew the password for the system administrator usercode.

(2) Four individuals had administrator access rights that exceeded their job responsibilities.

Misuse of the administrator usercode and the administrator access rights could result in unauthorized access to data and system files on the LAN and a lack of accountability.

g. The Department did not effectively restrict access to network resources. We reviewed access rights to several system level directories and noted:

(1) The Department did not restrict supervisor access rights* to network administrators. Misuse of supervisor access rights could result in unauthorized access to data and system files on the LAN.

(2) The Department did not effectively limit users' access to system level files and application programs. Access should be granted only to the extent needed to perform job duties. Limiting access would reduce the risk of unauthorized access and changes to system files on the LAN.

h. The Department did not activate the audit log feature to monitor sensitive network activity. An audit log records the activity performed by specific users. For example, network administrators perform and manage sensitive network activity that could be recorded in the audit log. The Department should identify sensitive activity and develop methods to monitor it.

RECOMMENDATION

We recommend that the Department establish effective LAN user access controls over data and application program files.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and responded that it has taken action to establish effective LAN user access controls and that it expects to be completed by July 30, 2000.

FINDING

3. LAN Physical Security Controls

The Department had not established effective physical security controls over LAN resources.

* *See glossary at end of report for definition.*

Effective physical security controls would help ensure that valuable network resources are safeguarded and that access is limited to individuals responsible for managing the network. Our review of physical security controls identified the following:

a. Access to the file server room was controlled by a combination keypad, but the Department was unable to provide us with a list of all individuals who knew the combination for the keypad. The Department should establish a list of authorized users and periodically change the combination to reduce the likelihood of unauthorized access to network resources.

b. The Department did not monitor access to its telephone closets where the LAN connections are located. DMB owns the closets and shares them with the Department for network use. As a result, the Department has difficulty controlling or monitoring access to its network connections. The Department should assess the risk of unauthorized access to its network via the telephone closets.

c. The Department did not have fire detection and fire prevention devices in the server room. Such devices would help to protect the LAN resources in the event of a fire.

RECOMMENDATION

We recommend that the Department establish effective physical security controls over LAN resources.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us it has changed the combination of its server room, limited independent access to the server room, and initiated a log-in for other personnel. In addition, the Department will assess the risk of unauthorized access to its network via the telephone closets by December 30, 2000. Further, the Department will seek a recommendation for appropriate fire detection and prevention measures for its server room as part of an overall disaster avoidance and recovery program.

FINDING

4. LAN Backup and Recovery Controls

The Department had not established effective LAN backup and recovery controls.

Effective LAN backup and recover controls ensure that LAN applications can be restored in the event of a disaster. We reviewed backup and recovery controls over the LAN and found:

a. The Department did not store all onsite LAN backup files in a secure location.

b. The Department had not completed and tested a written plan for recovering the LAN from backup files and restoring data and programs in the event of a disaster.

Data and programs can be lost through human error, equipment malfunction, and natural disasters. Without adequate planning and testing, restoring backup files and recovering from a disaster could be extremely costly and time consuming, if not impossible, and could significantly impair Department operations.

RECOMMENDATION

We recommend that the Department establish effective LAN backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us that it has secured its on-site LAN backup files. The Department expects to document and periodically test its backup and recovery procedures by September 30, 2000.

FINDING

5. Software Licensing Agreements Controls

The Department had not established effective controls to help ensure compliance with software licensing agreements.

DMB Administrative Guide procedure 1310.02 requires the central identification and inventory of all software. This is to ensure compliance with software license agreements.

The Department did not provide for the central identification and inventory of authorized software used by the Department. Also, the Department did not periodically review compliance with software license agreements. Violations of software licensing agreements could result in damage claims from software manufacturers.

RECOMMENDATION

We recommend that the Department establish effective controls to help ensure compliance with software licensing agreements.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us that it has begun the process to inventory all of its software licenses and that it expects to be completed by September 30, 2000. In addition, the Department will install server-based software to review compliance with software agreements by December 30, 2000 and conduct random workstation compliance reviews beginning April 1, 2000.

FINDING

6. Program Change Controls

The Department had not established effective program change controls.

Establishing controls over the modification of application software programs helps ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Our review of program change controls noted the following:

a. All of ITSD's programmers and analysts had access to client-server production source code. Some of those same employees had write and copy access to the

production executable directory. As a result, an employee could make changes to a program and move it into production without the appropriate approvals or testing.

b. The Department did not have a mechanism in place for programmers to check in and check out production source code and to log and monitor when the source code was copied or changed. Controlling access to application programs is critical to prevent unauthorized changes or replacement.

c. The Department did not maintain previous versions of client-server applications on the network. When ITSD moves a modified program into production, it writes over the old program. Currently, the only way to get a previous version is off the network backup tapes and those are only maintained for a year. Without maintaining previous program versions that can serve as an audit trail, the project's developer cannot re-create a previous version of the file and the project's history.

d. The Department had not developed written procedures detailing the program change process for its client-server systems. Procedures help ensure proper management and control over changing application programs.

RECOMMENDATION

We recommend that the Department establish effective program change controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and will implement effective program change controls by September 30, 2000.

INTERNAL CONTROL OVER ELECTRONIC FILING OF TAX RETURNS

COMMENT

Background: The internal control over the electronic filing of tax returns consists of application controls that are primarily concerned with the processing of information. Collectively, they form a network of controls in an information processing system, which

helps produce reliable and secure information. Application controls are grouped according to the various stages of an information processing system: (a) data origination, (b) data input, (c) data processing, and (d) data output.

Audit Objective: To assess the effectiveness of the Department's internal control over the information system that supports electronic filing of tax returns.

Conclusion: The Department's internal control over the information system that supports electronic filing was reasonably effective. Our assessment did not disclose any material conditions; however, we noted reportable conditions related to JELF access controls and software approval procedures.

FINDING

7. JELF Access Controls

The Department had not established effective access controls for the JELF System.

We examined access controls over JELF application programs and data and noted the following:

a. The Department did not restrict access to JELF programs and data to only authorized users. We identified 75 userscodes with access to JELF application programs and databases beyond what was necessary to perform the users' job responsibilities. We also identified 19 users with the capability to modify electronically filed tax return data while it was stored on a network directory prior to being uploaded into the JELF database* . Ensuring the integrity of the data before and after it is uploaded into the database is extremely important. The Department should reassess access rights to income tax records.

b. The Department did not monitor individual access into the JELF database. We noted that authorized users shared two common usercodes and passwords. These usercodes and passwords were also accessible by individuals who did not need this access to perform their job responsibilities.

* *See glossary at end of report for definition.*

Individuals should be assigned unique usercodes in order to maintain accountability.

Also, the Department did not use a database audit log. An audit log records the activity of specific users of the database. DMB Administrative Guide procedure 1310.02 requires that security violations be logged, the logs be reviewed, and problems be resolved. The database audit log along with unique usercodes would allow management to monitor security and maintain accountability.

c. The Department did not implement proper separation of duties. The JELF database administrator also wrote the application programs. Separating the functions of the database administrator and programmer would help ensure proper controls over program changes and data integrity.

RECOMMENDATION

We recommend that the Department establish effective access controls for the JELF system.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and will appropriately adjust access to the JELF database by June 30, 2000. The Department also informed us that, as of March 1, 2000, it established unique usercodes for each JELF user in order to maintain accountability. Further, the Department informed us that it is in the process of training new developers so that division of duties can be assessed.

FINDING

8. Software Approval Procedures

The Department did not have written procedures for reviewing and approving electronic tax return software.

The Department only accepted electronic returns submitted with approved software. For software to become approved, developers have to submit test tax returns according to Department specifications. The Department compares a

developer's test data with the specifications. Once the developer submits all State test tax returns accurately and the Internal Revenue Service (IRS) accepts the software developer's federal test returns, the Department approves the software for use in electronically submitting State tax returns.

We reviewed the test results of 2 of the 20 developers. We found instances in both cases in which the developers' test data did not match the Department's specifications, but the Department approved the software anyway. For one of the test tax returns, both developers submitted the same incorrect data and one developer's data was accepted and the other's was not. In these cases, the differences between developers' test data and the Department specifications were insignificant. However, the Department did not have any written procedures explaining the approval process and the type of differences deemed insignificant. As a result, employees reviewing the test results used their own judgment to determine if a difference was significant. Written procedures would help ensure that reviewers are making consistent and accurate determinations regarding the significance of the differences in the developers' test data from the specifications.

RECOMMENDATION

We recommend that the Department develop written procedures for reviewing and approving electronic tax return software.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us that it has begun to write procedures for reviewing and approving third parties' electronic filing software.

INTERNAL CONTROL OVER THE RECONCILIATION OF BANK ACCOUNTS AND THE STATE'S ACCOUNTING RECORDS

COMMENT

Background: Internal control of the RECON-Plus System consists of application controls that are primarily concerned with the processing of information. Collectively, they form a network of controls in an information processing system, which helps

produce reliable and secure information. Application controls are grouped according to the various stages of an information processing system: (a) data origination, (b) data input, (c) data processing, and (d) data output.

Audit Objective: To assess the effectiveness and efficiency of the Department's internal control over the information system used to reconcile bank accounts with the State's accounting records.

Conclusion: The internal control over the Department's system used to reconcile bank accounts with the State's accounting records was reasonably effective. Our assessment did not disclose any material conditions; however, we noted reportable conditions related to RECON-Plus user access controls and RECON-Plus system documentation.

FINDING

9. RECON-Plus User Access Controls

The Department had not established effective access controls over RECON-Plus.

Effective access controls protect assets, establish accountability, and limit access to the extent necessary for employees to perform their jobs while maintaining the integrity of the system.

Our review of the authorized users disclosed:

a. The Department created a usercode with administrator access rights that all users of the system shared. Administrator access rights allow a user to access all capabilities of RECON-Plus, including the ability to create new users and establish and edit match criteria. Access rights should be granted only to the extent necessary for employees to perform their jobs, and shared usercodes should be prohibited to maintain accountability.

b. The accountants copy bank and accounting data into RECON-Plus to facilitate the reconciliation process. The accountants' access rights allow them to alter this data, which puts the integrity of the bank and accounting data at risk. The Department informed us that the accountants needed this access to correct

data input errors. The Department should establish compensating controls, such as monitoring the RECON-Plus audit trail.

c. RECON-Plus cannot prevent unauthorized access to its database through other application software. The Department informed us that the software manufacturer is aware of this risk and is working towards a resolution. In the meantime, the Department should develop compensating controls, such as monitoring the database audit log, to detect unauthorized access.

RECOMMENDATION

We recommend that the Department establish effective access controls over RECON-Plus.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed us that it has removed the shared usercode from the system and that it will establish methods to monitor accountants' corrections to bank and accounting data. In addition, the Department informed us that the software manufacturer is working to correct access control risks and that it will establish compensating controls for maintaining the integrity of the RECON-Plus database.

FINDING

10. RECON-Plus System Documentation

The Department should continue its efforts to complete system documentation for RECON-Plus.

System documentation provides an understanding of processes, data, and controls. It defines the system objectives and provides a means to ensure that the system operates as intended. System documentation should describe how the system operates and how the user interacts with the system:

a. The Department should complete system narratives and flowcharts for the cash reconciliation process. The Department did document the portion of the system

developed by ITSD, but did not document the entire process. Lack of system documentation could result in higher system maintenance costs.

b. The Department should complete data processing policies and procedures for the cash reconciliation process, including those for importing data, and preparing and distributing the final reconciliation report. Policies and procedures communicate to staff the extent of their responsibilities and minimize the impact of staff turnover on system operations.

RECOMMENDATION

We recommend that the Department continue its efforts to complete system documentation for RECON-Plus.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation and informed that us that it will complete documentation for RECON-Plus.

Glossary of Acronyms and Terms

approved tax software	Software that has passed the State's testing requirements for filing electronic income tax returns.
client-server	An architecture in which one computer can get information from another. The client is the computer that asks for access to data, software, or services. The server, which can be anything from a personal computer to a mainframe, supplies the requested data or services for the client.
DMB	Department of Management and Budget.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical for the amount of resources applied or minimizing the amount of resources required to attain a certain level of outputs or outcomes.
internal control	The management control environment, management information system, and control policies and procedures established by management to provide reasonable assurance that goals are met; that resources are used in compliance with laws and regulations; and that valid and reliable performance related information is obtained and reported.
IRS	Internal Revenue Service, U.S. Department of Treasury.
ITSD	Information Technology Services Division.
JELF database	A database containing the electronically filed tax return data elements.

Joint Electronic Filing (JELF) System	A client-server system used by the Department of Treasury for processing, storing, and retrieving electronically filed Michigan income tax returns.
local area network (LAN)	A group of computers connected to each other over a small geographical area, such as a building or office, for the purpose of sharing hardware, software, and information.
material condition	A serious reportable condition which could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the opinion of an interested person concerning the effectiveness and efficiency of the program.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
RECON-Plus System	A client-server software package designed for automatically reconciling transactions.
reportable condition	A matter coming to the auditor's attention that, in the auditor's judgment, should be communicated because it represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
supervisor access rights	Grant all rights to a directory, its files, and its subdirectories. These rights include the ability to read, write, create, erase, modify, and grant others access to directories and files. Supervisor access rights override any restrictions placed on subdirectories or files. Users who have this right in a directory can grant other users supervisor access rights to the directory, its files, and its subdirectories.